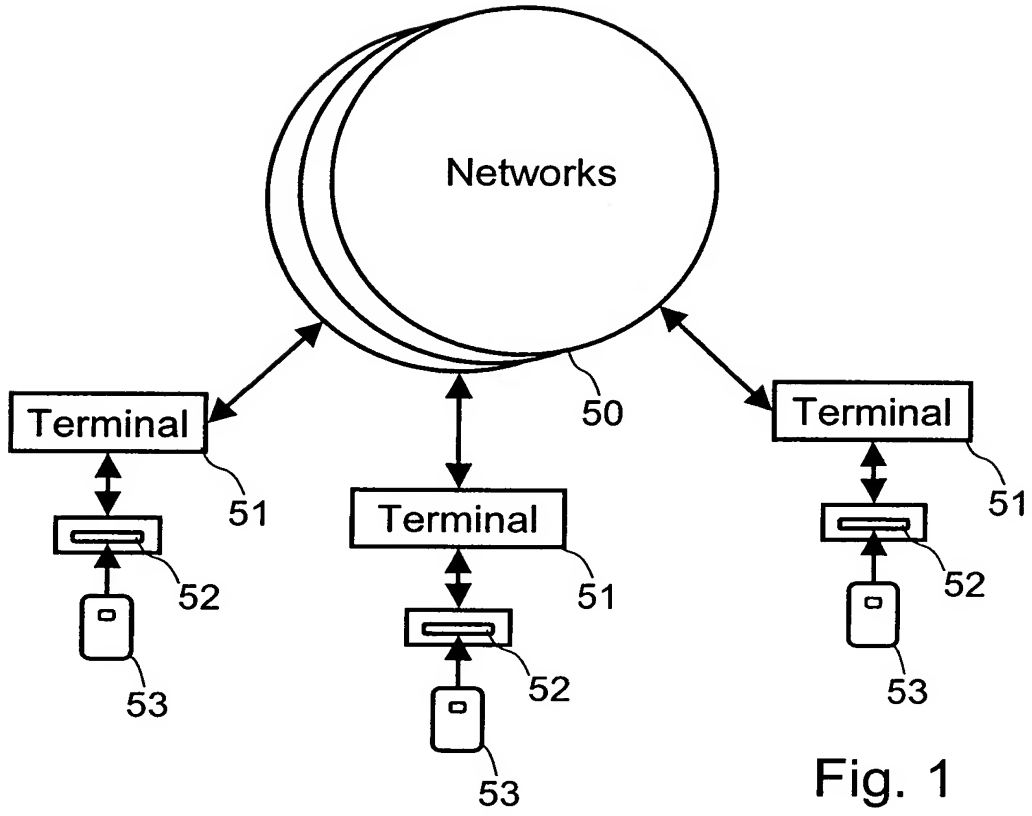

Fig. 1

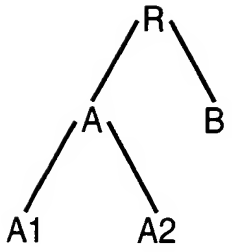

Fig. 2

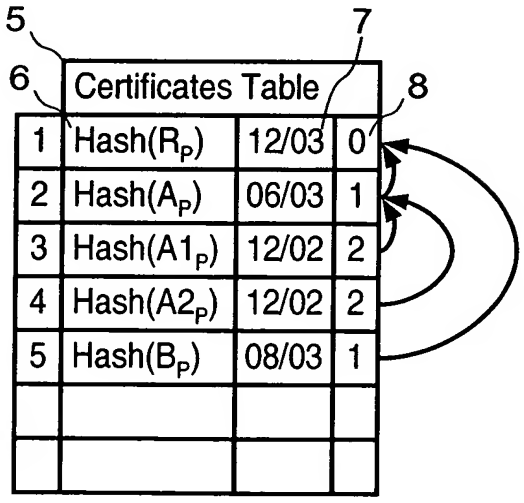

Fig. 3

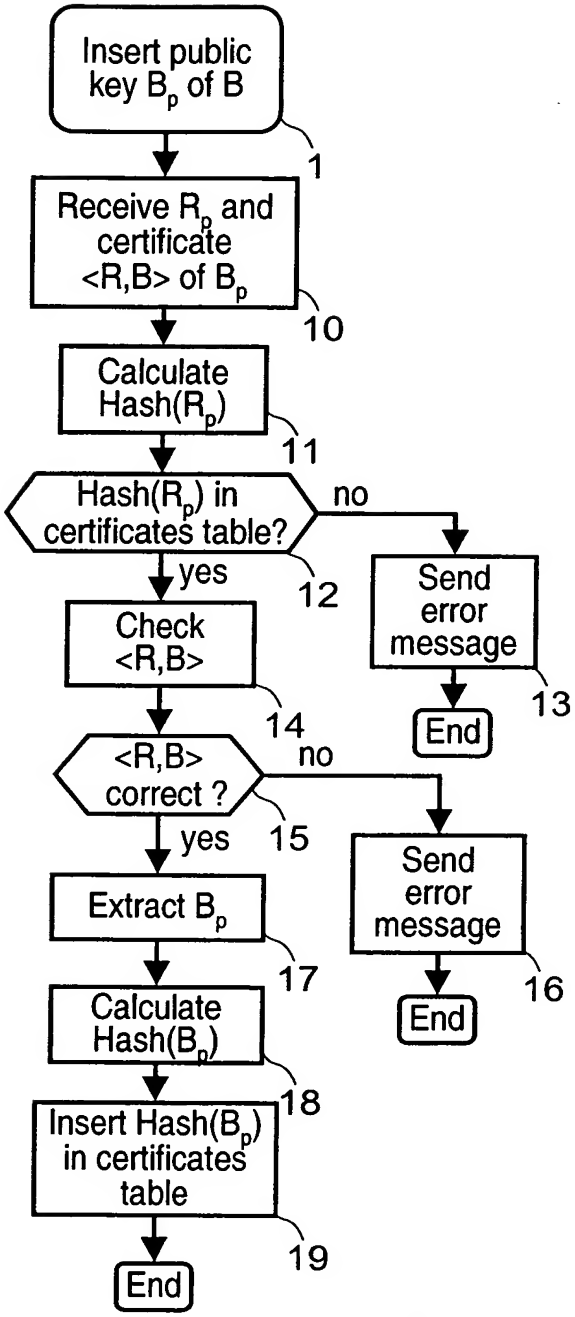
Insert public key B_p of B
1
Receive R_p and certificate <R,B> of B_p
10
Calculate Hash(R_p)
11
Hash(R_p) in certificates table?
no
12
yes
Send error message
13
End
Check <R,B>
14
<R,B> correct ?
no
15
yes
Send error message
16
End
Extract B_p
17
Calculate Hash(B_p)
18
Insert Hash(B_p) in certificates table
19
End

Fig. 4

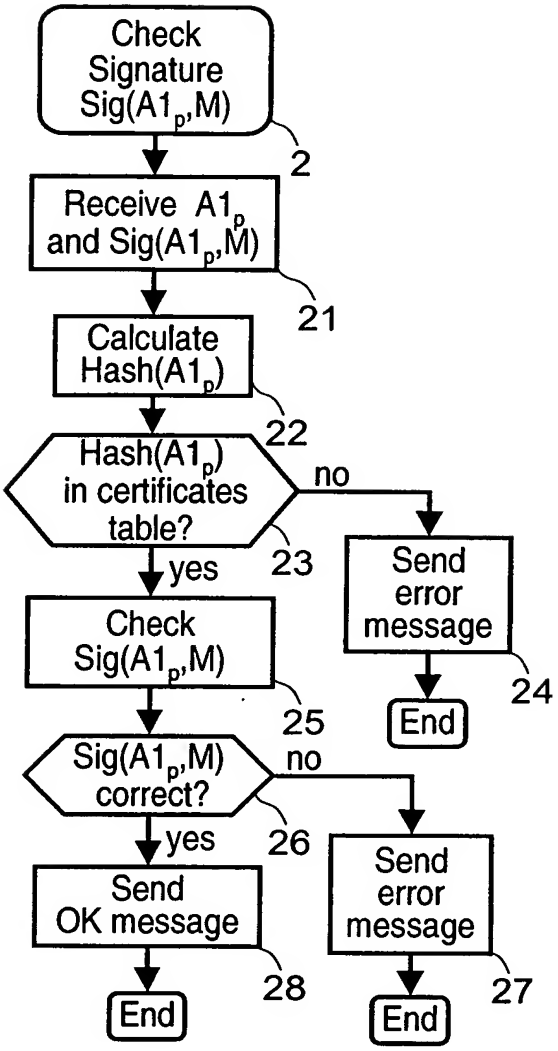
Check Signature Sig($A1_p$,M)
2
Receive $A1_p$ and Sig($A1_p$,M)
21
Calculate Hash($A1_p$)
22
Hash($A1_p$) in certificates table?
no
23
yes
Send error message
24
End
Check Sig($A1_p$,M)
25
Sig($A1_p$,M) correct?
no
26
yes
Send error message
27
End
Send OK message
28
End

Fig. 5

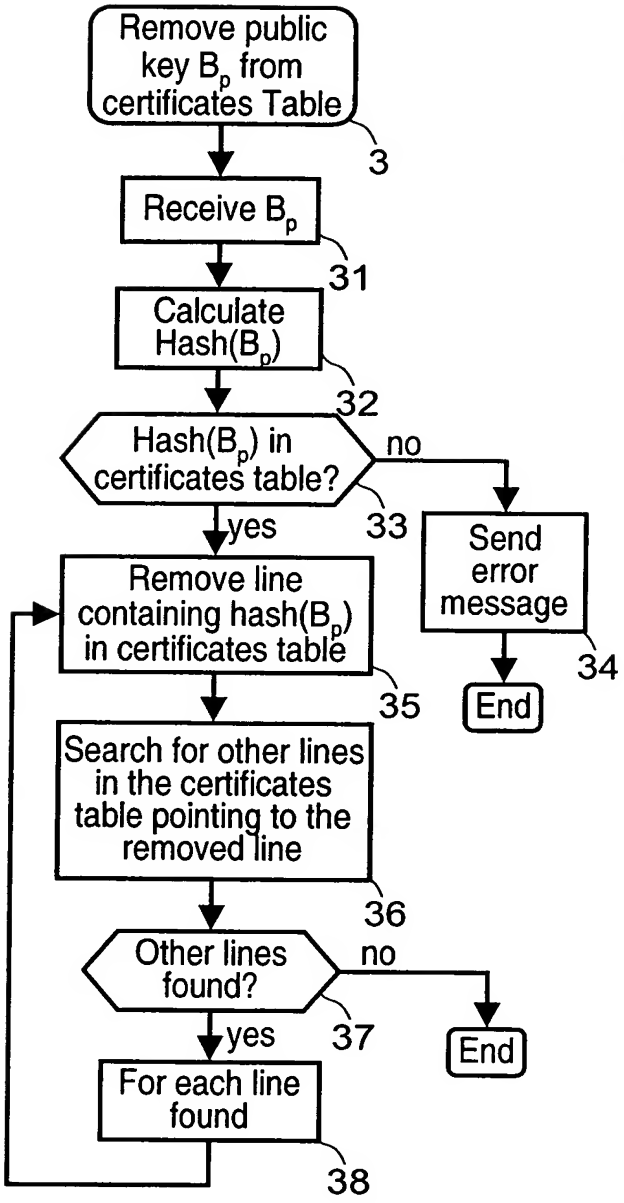
Remove public key B_p from certificates Table
3
Receive B_p
31
Calculate Hash(B_p)
32
Hash(B_p) in certificates table?
33
no
yes
Send error message
34
End
Remove line containing hash(B_p) in certificates table
35
Search for other lines in the certificates table pointing to the removed line
36
Other lines found?
37
no
yes
End
For each line found
38

Fig. 6

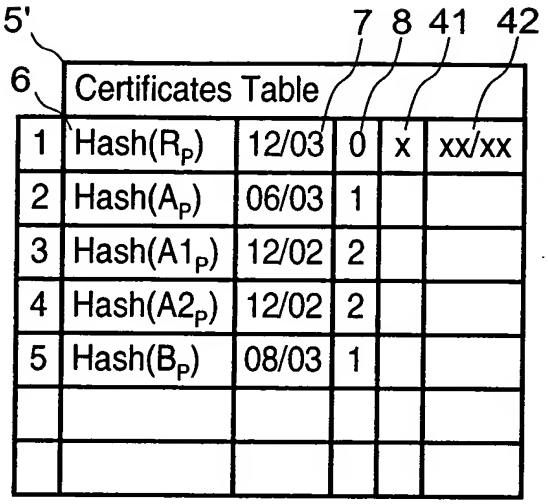
5'
7
8
41
42
6
Certificates Table
1 Hash(R_P) 12/03 0 x xx/xx
2 Hash(A_P) 06/03 1
3 Hash($A1_P$) 12/02 2
4 Hash($A2_P$) 12/02 2
5 Hash(B_P) 08/03 1

Fig. 7